REMARKS

The Office Action dated January 19, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 18, 20-22, 24, 26-41, and 45-48 are amended to more particularly point out and distinctly claim the subject matter of the present invention and to correct typographical informalities. No new matter is added. Claims 1-48 are respectfully submitted for consideration.

The Office Action objected to claims 22, 24, 26, 27, 29, 31 and 35 because of typographical informalities. Applicants submit that all known typographical errors have been corrected. Accordingly, withdrawal of the objection to the claims is respectfully requested.

The Office Action rejected claims 2, 20, 28-30, 32, 33, 36-41 and 45-47 under 35 U.S.C. 112, second paragraph for being indefinite. Applicants respectfully submit that the "wherein" clauses of each of these claims are amended to be more definite. Regarding claim 2 the phrase referred to in the Office Action is recited in claim 22. Accordingly, withdrawal of the rejection under 35 U.S.C. 112, second paragraph is respectfully requested.

The Office Action rejected claims 1-5, 8-15, 19, 21, 22-26, 29, 31, 32, 34, 35-38, 42-44, 46 and 48 under 35 U.S.C. 102(e) as being anticipated by US Patent No. 7,058,970 to Shaw (Shaw). This rejection is respectfully traversed.

Claim 1, from which claims 2-8 depend, is directed to an apparatus for verifying the security integrity of remote network devices. A proxy device receives a request for network services by at least one remote network device and performing a security integrity scanning operation on the requesting remote network device. An authorization processing unit and access control rules unit determine if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

Claim 9, from which claims 10-21 depend, is directed to a system for verifying security integrity of remote network devices. At least one remote network device accesses a network via a network connection to make a request for one or more network resident services. A gateway device receives the request for services and performing a security integrity scanning operation on the remote network device prior to allowing access to the requested network services. An authentication server verifies user authentication credentials of users of remote network devices that access the network. At least one network server provides requested network services to at least one remote network device accessing the network through the gateway device.

Claim 22, from which claims 23-34 depend, is directed to a method for verifying security integrity of remote network devices. At least one variable used as a vehicle is defined to convey the results of the scanning process. Verification software is downloaded via a network connection to the remote network device that performs scanning process and reports result used in scanning script, including at least one

variable. At least one scanning operation is performed on the remote network device to verify the security integrity of the remote device. The results of the scanning operation are obtained for purposes of determining whether or not the remote network device is authorized to access the requested network services.

Claim 35, from which claims 36-48 depend, is directed to a method for assessing the integrity of remote network devices for purposes of regulating access to network services via a network gateway. At least one access control policy is defined for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on the remote network device. Verification software is downloaded that an administrator can specify what scan scripts are used under what conditions to the remote network device. An integrity scan is performed on the remote network device. At least one result of the scan is conveyed to a gateway device. Access by the remote network device is regulated to network services via the gateway device based, at least in part, on the results of the integrity scan.

According to certain embodiments of the presently claimed invention, whenever the user of the network device requires access to the network servers proxied by the gateway the gateway determines whether the user is authorized to access the service requested. The authorization is done on a per service basis using the authorization processing unit and the access control rules unit. Access control rules unit contains access controls that specify actions based on variables that are given values when a remote network device signs on when integrity scans occur. One of the benefits of the client

integrity scanning of the present invention is that the gateway can be configured to prevent a user from accessing the gateway sign on page from a remote device that may have already been compromised by an attacker. Therefore, the user can avoid entering enterprise passwords on insecure remote devices. Applicants submit that each of the pending claims recites features that are neither disclosed nor suggested in Shaw.

Shaw is directed to a network security authority system that provides on-connect scan and delivery in a virtual lobby to enforce security requirements for a network. One embodiment of a network security authority includes two firewalls around a virtual lobby. The example described in Shaw considers a physical lobby in a building. It has doors locked during certain hours, a guard checking badges, briefcases, and packages, and other physical security. Like the physical lobby protects the building, the virtual lobby protects a network from potentially insecure connections. The virtual lobby includes at least one computing system and one or more software components capable of causing the computing system(s) to operate to protect the network. The virtual lobby protects the network from many threats, such as a client that has picked up a worm while surfing the Internet or a client that does not know it has a virus with the potential to spread it to the network. The virtual lobby ensures that any client that connects into the network has certain types of protection, such as proper virus protection software in order to avoid risks like spreading viruses.

Applicants respectfully submit that Shaw fails to disclose or suggest at least the features of a proxy device for receiving a request for network services by at least one

remote network device and performing a security integrity scanning operation on the requesting remote network device, and determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation, as recited in clam 1 and similarly recited in claims 9, 22 and 35.

Shaw merely discloses that the client accesses the log on page whereby the client does not get into the network if they do not have the correct user identification and password to log in. Therefore, in the arrangement of Shaw it is still possible that the gateway sign on page can be accessed from a remote device that has already been compromised by an attacker. Therefore should the correct enterprise passwords be entered access will be gained by an insecure remote device.

Applicants submit that because claims 2-5, 8, 10-15, 19, 21, 23-26, 29, 31, 32, 34, 36-38, 42-44, 46 and 48 depend from claims 1, 9, 22 and 35, these claims are allowable at least for the same reasons as claims 1, 9, 22 and 35, as well as for the additional features recited in these dependent claims.

Based at least on the above, Applicants respectfully submit that Shaw fails to disclose or suggest all of the features of claims 1-5, 8-15, 19, 21, 23-26, 29, 31, 32, 34-38, 42-44, 46 and 48. Accordingly, withdrawal of the rejection under 35 U.S.C. 102(e) is respectfully requested.

The Office Action rejected claims 6, 7, 16-18, 27, 28, 30, 40, 41 and 45 under 35 U.S.C. 103(a) as being obvious over Shaw, in view of US Patent No. 6,728,886 to Ji et al. (Ji). The Office Action took the position that Shaw disclosed most of the features of

these claims except a signed applet, executing the script allowed to access the remote device for the purposes of executing programs as well as searching and reading specific data filed that reside on the remote network device. The Office Action asserted that Ji disclosed these features. Applicants submit that the cited references taken individually or in combination, fail to disclose or suggest all of the features of any of the above claims. Specifically, Shaw is deficient at least for the same reasons discussed regarding claims 1, 9, 22, and 35, and Ji fails to cure these deficiencies.

Shaw is discussed above. Ji is directed to detecting viruses that may be transferred between a distributed computer network, such as the Internet, and a host computer. A host computer performs its own virus scanning on data, using executables code downloaded to its browser upon a request for data from the Internet, such as an HTTP request. Code is downloaded to the host computer, and is configured to create a virus scan module on the host computer upon such a request. The module is used to detect viruses in data transferred between the host computer and the Internet. Virus scanning is performed thereafter on the host computer. In cases where certain browsers may not be capable of supporting local virus scanning, code is first downloaded to determine whether local scanning is possible. If so, the virus scan module is then downloaded and executed.

However, as discussed above, embodiments of the presently claimed invention prevent sign on pages being accessed by compromised insecure remote devices (paragraph [0031] of published version of current application). This feature is neither disclosed nor suggested in Shaw. Furthermore, Ji fails to cure these deficiencies.

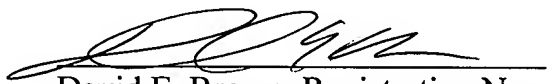
Based at least on the above, Applicants submit that the cited references fail to disclose or suggest all of the features of claims 6, 7, 16-18, 27, 28, 30, 40, 41 and 45. Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

Applicants submit that each of claims 1-48 recite features that are neither disclosed nor suggested in any of the cited references. Accordingly, it is respectfully requested that each of claims 1-48 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown, Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14TH Floor
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800; Fax: 703-720-7802
DEB:jkm